UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/702,167	11/05/2003	Nancy Cam Winget	72255/00006	7272

23380 7590 11/27/2009

TUCKER ELLIS & WEST LLP
1150 HUNTINGTON BUILDING
925 EUCLID AVENUE
CLEVELAND, OH 44115-1414

EXAMINER	
DEBNATH, SUMAN	

ART UNIT	PAPER NUMBER
2435	

NOTIFICATION DATE	DELIVERY MODE
11/27/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patents@tuckerellis.com

Office Action Summary	Application No.	Applicant(s)	
	10/702,167	WINGET ET AL.	
	Examiner	Art Unit	
	SUMAN DEBNATH	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 July 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16 and 28-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16 and 28-30* is/are rejected.

7)☒ Claim(s) *1, 9, 28 and 29* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-16 and 28-30 are pending in this application.

2. Claims 1 and 9 are currently amended.

3. Claims 17-27 are canceled.

4. Claims 29-30 are newly added.

5. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office Action.

Continued Examination Under 37 CFR 1.114

6. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on July 10, 209 has been entered.

Claim Objections

7. Claims 1, 9, 28 and 29 are objected to because of the following informalities:

As to claim 1, it recites, "the server encryption key" and "the server authentication key" in line 6; “the peer encryption key” and “the peer authentication key" in line 8; “the same encryption and authentication keys” in line 10; there is insufficient antecedent basis for these limitations in the claim.

As to claim 9, it recites, "the server encryption key" and "the server authentication key" in line 7; "the peer encryption key" and "the peer authentication key" in line 9; "the same encryption and authentication keys" in line 11;there is insufficient antecedent basis for these limitations in the claim.

As to claim 28, it recites, "the group consisting of establishing the secure tunnel" in line 2. There is insufficient antecedent basis for this limitation in the claim.

As to claim 29, it recites, "the Diffie-Helman tunnel" in line 2. There is insufficient antecedent basis for this limitation in the claim.

Appropriate correction and/or clarifications are required.

Claim Rejections - 35 USC § 101

8. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

9. Claims 9-16 are rejected under 35 U.S.C 101 because the claims are directed to non-statutory subject matter.

As to claim 9, the language of the claim(s) raises a question whether the claim is directed merely to an abstract idea that is not tied to an environment or machine which would result in a practical operation producing a concrete, useful, and tangible result to form the basis of statutory subject matters under 35 U.S.C 101. The claim recites, "an implementation for enabling secure communication comprising:" followed by "an implementation for establishing a secure tunnel" in line 3, "an implementation for authenticating" in line 5, "an implementation for hashing" in line 7, "an implementation

for hashing" in line 9, "an implementation for verifying" in line 11, "an implementation for providing" in line 13 and "an implementation for signaling" in line 16. It's not clear from the Specification whether these implementations are software and/or hardware implementations. Anybody with ordinary skill in the art would understand that these functionalities (i.e. authenticating, hashing, verifying) are mostly implemented as software modules. Thus, Examiner asserts that these implementations are software implementations that direct the claim to non statutory subject matter (i.e. software per se).

As to claims 10-16, they are rejected because of their dependency on claim 9, and further not being able to tie to an environment or machine which would result in a practical operation producing concrete, useful and tangible results.

Appropriate correction and/or clarifications are required.

Claim Rejections - 35 USC § 103

10. Claims 1-16 and 28-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Funk (Paul Funk; Simon Blake-Wilson; "draft-ietf-pppext-eap-ttls-02.txt: EAP Tunneled TLS Authentication Protocol (EAP-TTLS)"; Internet-Draft PPPEXT Working Group; Nov. 2002, p. 1-40) (hereinafter "Funk") and further in view of Bugnon et al. (Patent No.: US 6,397,056 B1) (hereinafter, "Bugnon") and Spies et al. (Patent No.: US RE38,070 E) (hereinafter, "Spies").

11. As to claim 1, Funk discloses a method of secure communication comprising:

establishing a secure tunnel between a server and a peer using an encryption algorithm that establishes an encryption key (pages 9-10, section 4.3; pages 11-13, sections 6-6.2);

authenticating the peer with the server over the secured tunnel establishing an authentication key (pages 9-10, section 4.3; pages 11-13, sections 6-6.2 and page 20, section 10);

verifying by the server that the peer possesses the same encryption and authentication keys as the server (pages 9-10, section 4.3; pages 11-13, sections 6-6.2; and page 20, section 10);

provisioning a network access credential to the peer using the secured tunnel, responsive to the verifying the peer possesses the same encryption and authentication keys as the server ("The keying material is developed implicitly between client and TTLS server based on the results of the TLS handshake; the TTLS server will communicate the keying material to the access point over the carrier protocol" –e.g. page 12-13, sections 6-6.2, see also pages 9-10, section 4.3; pages 11-16, section 6-7, page 20, section 10);

Funk is silent on hashing the server encryption key and the server authentication key to produce a first hash; hashing the peer encryption key and the peer authentication key to produce a second hash; and verifying by comparing the first hash with the second hash; signaling an authorization failure to the peer conclusion of the provisioning of the network access credential, prior to the peer authenticating using the

provisioned credentials, and denying the peer access to the network by the server until the per authenticates using the provisioned credentials.

However, Bugnon discloses signaling an authorization failure to the peer conclusion of the provisioning of the network access credential, prior to the peer authenticating using the provisioned credentials, and denying the peer access to the network by the server until the per authenticates using the provisioned credentials (col. 6, lines 17-37, Bugnon teaches this concept by having authentication failure messages until a positive authentication is made, see also, FIG. 3B, col. 7, lines 57-67, col. 8, lines 20-45).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Funk as taught by Bugnon in order to identify legitimate user that is authorized to use a service.

Neither Funk nor Bugnon explicitly disclose hashing the server encryption key and the server authentication key to produce a first hash; hashing the peer encryption key and the peer authentication key to produce a second hash; and verifying by comparing the first hash with the second hash.

However, Spies discloses hashing the server encryption key and the server authentication key to produce a first hash; hashing the peer encryption key and the peer authentication key to produce a second hash; and verifying by comparing the first hash with the second hash (It should be noted that using hash function during authentication process is well known in the art. Spies teaches the above concept by recalculating hash

on the server side and if the two hashes matches, server assured authorization, e.g. see, col. 11, lines 1-10, see also, col. 9, lines 24-36).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Funk and Bugnon as taught by Spies in order to increase the integrity of the authorization process by make use of the well known hashing function.

12. As to claim 9, it is rejected using the similar rationale as for the rejection of claim 1.

13. As to claims 2 and 10, the combination of Funk, Bugnon and Spies disclose wherein the communication implementation between the at least first and second parties is at least one of a wired implementation and a wireless implementation (Funk: pages 4-5, section 2).

14. As to claims 3 and 11, the combination of Funk, Bugnon and Spies disclose wherein the encryption algorithm is an asymmetric encryption algorithm (Funk: page 9-10; sections 4.2-4.3; page 28, section 12).

15. As to claims 4 and 12, the combination of Funk, Bugnon and Spies disclose wherein the asymmetric encryption algorithm is used to derive a shared secret,

subsequently used in the step of establishing a secure tunnel (Funk: page 9-10; sections 4.2-4.3; page 28, section 12).

16. As to claims 5 and 13, the combination of Funk, Bugnon and Spies disclose wherein the asymmetric encryption algorithm is Diffie-Hellman key exchange (Funk: pages 36-37, section 14).

17. As to claims 6 and 14, the combination of Funk, Bugnon and Spies disclose wherein the step of authenticating is performed using Microsoft MS-CHAP v2 (Funk: pages 11-12; section 6; pages 23-24, section 10.2.4).

18. As to claims 7 and 15, the combination of Funk, Bugnon and Spies disclose further comprising a step of provisioning a public/private key pair on one of the at least server and peer, and then to provision that public key on the respective remaining ones of the at least server and peer (Funk: pages 11-16, sections 6-7).

19. As to claims 8 and 16, the combination of Funk, Bugnon and Spies disclose wherein the step of provisioning a public/private key pair comprises providing a server-side certificate in accordance with Public Key Infrastructure (PKI) (Funk: pages 9-10, sections 4.2-4.3, page 20, section 10).

20. As to claim 28, Funk discloses further comprising invalidating a secure credential for the second party responsive to a failure of one of the group consisting of establishing the secure tunnel, authentication, and verifying second party has the same encryption and authentication keys ("If either item does not match exactly, the TTLS server must reject the client" –e.g. page 23).

21. As to claim 29, Funk discloses further comprising: detecting a man-in-the-middle attack over the Diffie-Helman tunnel; and selecting an alternate asymmetric encryption algorithm responsive to detecting the attack (Funk: pages 9-10, sections 4.2-4.3, page 20, section 10).

22. As to claim 30, Funk discloses wherein the Diffie-Helman key exchange is one of server-authenticated or anonymous (Funk: pages 9-10, sections 4.2-4.3, page 20, section 10).

23. Examiner's note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the Applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may be applied as well. It is respectfully requested from the Applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part

of the claimed invention as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

Response to Arguments

24. Applicant's arguments with respect to claims 1 and9 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

25. Any inquiry concerning this communication or earlier communications from the examiner should be directed to SUMAN DEBNATH whose telephone number is (571)270-1256. The examiner can normally be reached on 8 am to 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/S. D./
Examiner, Art Unit 2435

/Kimyen Vu/

Supervisory Patent Examiner, Art Unit 2435